



НАО «Атырауский университет имени Халела Досмухамедова»

ПОЛОЖЕНИЕ



УТВЕРЖДАЮ

Председатель Правления-ректор
НАО Атырауского университета
имени Х.Досмухамедова

С.Н.Идрисов
«2» 09 2024 г.

**ПОЛОЖЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С
АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)**

№223

Атырау 2024г.

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 2 из 13

	Должность	Ф.И.О.	Подпись	Дата
Разработал	Руководитель Центра разработки и развития ИКТ	Мендигалиев.Ж.Ж.		25.08.24
Согласовано	Проректор по академическим вопросам	Чукуров А.Е.		2.09.24
Согласовано	Вице-проректор (цифровой офицер)	Сулейменова Ж.У		26.08.24
Согласовано	Руководитель офис мониторинга качества	Кайшыгулова Ж.Т.		24.08.24
Согласовано	Юрист	Куанов К.С.		28.08.2024.

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 3 из 13

СОДЕРЖАНИЕ

1.	Общие Положения	4
2.	Нормативные ссылки	6
3.	Термины и определения	6
4.	Объекты информационной безопасности	8
5.	Организационно-правовой статус ответственного лица за информационную безопасность и системное администрирование	8
6.	Требования к информационной безопасности	8
7.	Требования по аутентификации пользователей в системе	9
8.	Пересмотр положения	10
9.	Ответственность	10
10.	Заключительное положение	11
11.	Лист регистрации изменений и дополнений	13

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 4 из 13

1. Общие положения

- 1.1. Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированная информационная системы «Platonus» (далее – АИС) в Атырауском университете имени Халела Досмухамедова (далее – Атырауский университет), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с логином и паролями.
- 1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации Атырауского университета.
- 1.3. Положение является методологической базой для:
- 1)выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
 - 2)обеспечения информационной безопасности;
 - 3)координации деятельности структурных подразделений университета при проведении работ по соблюдению требований обеспечения информационной безопасности.
- 1.4. Требования и условия настоящего Положения применяются в отношении всех информационных систем университета.
- 1.5. Настоящее Положение разработано с учетом текущего состояния и ближайших перспектив развития информационно-коммуникационной инфраструктуры (далее - ИКИ) университета. В положении описаны цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности.
- 1.6. Основные цели Положения:
- 1)доступность обрабатываемой информации;
 - 2)устойчивое функционирование ИКИ университета;
 - 3)обеспечение конфиденциальности информации, хранящейся, обрабатываемой средствами вычислительной техники и передаваемой по каналам связи;
 - 3)целостность и аутентичность информации, хранящейся и обрабатываемой в информационных системах университета и передаваемой по каналам связи.
- 1.7. Для достижения целей поставлены следующие задачи:
- 1)формирование и проведение единой политики в области обеспечения информационной безопасности в университете;
 - 2)обеспечение бесперебойной работы университета и сведение к минимуму экономического ущерба от реализации угроз информационной безопасности, посредством их предупреждения, предотвращения;
 - 3)определение процедур, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
 - 4)определение требований к содержанию процедур по управлению информатизацией в рамках университета с учетом необходимости решения задач по обеспечению информационной безопасности;
 - 5)координация деятельности университета при проведении работ в ИКИ с соблюдением требований стандартов обеспечения информационной безопасности;
 - 6)повышение уровня защищенности ИКИ университета;

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 5 из 13

1.8. Действие настоящего Положения распространяется на структурные подразделения университета, в которых осуществляется обработка информации, в том числе автоматизированная, содержащая административные данные, информацию с ограниченным распространением (служебная информация), или персональные данные, а также на организации, осуществляющие разработку, сопровождение, обслуживание функционирования информационной системы университета.

1.9. Область действия информационной безопасности других информационных систем определяется их владельцами. В случае если данные информационных систем состоят в ИКИ университета, условия информационной безопасности оговариваются в рамках договоров или совместных правилах взаимодействия между владельцем информационной системы и университетом.

1.10. К категориям пользователей ИС относятся:

1) внутренние пользователи - сотрудники университета, имеющие авторизованный доступ к ИР, осуществляющие свою деятельность и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;

2) внешние пользователи - потребители услуг университета, в том числе лица, использующие ИР университета;

3) вспомогательный персонал - обслуживающий, технический персонал и владельцы других ИС, осуществляющих взаимодействие в университете,

в том числе:

- администраторы ЛВС, ответственные за сопровождение телекоммуникационного оборудования;

- СА;

- разработчики ППО;

- инженеры-системотехники, технические специалисты (системно-техническое обслуживание) и др.

1.11. Требования настоящего Положения распространяются на всех работников структурных подразделений, профессорско-преподавательский состав и обучающий использующих в пользования АИС В университете.

1.12. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах Учреждения и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на специалистов Центра разработки и развития ИКТ (далее - специалист АИС) Учреждения.

1.13. Ознакомление всех работников Учреждения, использующих средства вычислительной техники, с требованиями Положения проводят руководители структурных подразделений. При ознакомлении с Положением внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации и утечки личной информации ППС состава и обучающихся университета.

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 6 из 13

2. Нормативные ссылки

- 1) Постановление Правительства Республики Казахстан от 20 декабря 2016 года №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
- 2) СНиП РК 2.02-05-2009 «Пожарная безопасность зданий и сооружений»;
- 3) СН РК 3.02-17-2011 «Структурированные кабельные сети. Нормы проектирования»;
- 4) СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;
- 5) СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения»;
- 6) СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;
- 7) СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защите информации»;
- 8) СТ РК ИСО/МЭК 27002-2009 «Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации».
- 9) СТ РК ИСО/МЭК 27002-2015 «Средства обеспечения. Свод правил по управлению защитой информации».

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении применены следующие термины, их определения и сокращения:

Информационная система (ИС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Информационная безопасность (ИБ) - обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности процесса и минимизации рисков.

Учетная запись - информация о пользователе АИС: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (ИИН, телефон и т.п.).

Принцип минимальных привилегий - принцип, согласно которому каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

Компрометация - утрата доверия к тому, что информация недоступна посторонним лицам.

Ключевой носитель - электронный носитель (флэш-накопитель, хард диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

Аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа, реализованными в системе;

База данных (БД) - совокупность данных, организованных согласно концептуальной структуре, описывающей характеристики этих данных, а также взаимосвязи между их объектами,

Градации информационной системы по уровням информационной безопасности - разделение информационной системы на классы по уровню предъявляемых к ним требований по обеспечению информационной безопасности;

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 7 из 13

Информационные ресурсы (ИР) – это совокупность данных: текст; графика; аудио; видео и др. хранящаяся в информационных системах.

Информационная система (ИС) – система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса;

Информационная безопасность (ИБ) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, не отказоустойчивости, подотчетности, аутентичности и достоверности информации или средства ее обработки;

Электронные информационные ресурсы (ЭИР) – электронные систематизированные массивы информации (информационные БД), содержащиеся в ИС, объединенные соответствующим программным обеспечением и представляющие интерес для пользователей информации;

Информационно-коммуникационная инфраструктура (ИКИ) – совокупность средств вычислительной техники, телекоммуникационного оборудования, каналов передачи данных и ИС, средств коммутации и управления информационными потоками;

Локально-вычислительная сеть (ЛВС) – сеть, объединяющая абонентов, расположенных в пределах небольшой территории;

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

Нормативные правовые акты (НПА) – письменный официальный документ установленной формы, принятый должностным(и) лиц(ом/ами), устанавливающий правовые нормы, изменяющий, прекращающий или приостанавливающий их действие, а также документ в электронно-цифровой форме, идентичный письменному официальному документу и удостоверенный посредством электронной цифровой подписи;

Пользователь ИС – субъект, обращающийся к ИС за получением необходимых ему электронных ИР и пользующийся ими;

Программное обеспечение (ПО) – совокупность компьютерных программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ;

Прикладное ПО (ППО) – ПО (или программа), которое предназначено для решения прикладной задачи;

Серверное помещение – помещение, предназначенное для размещения серверного, активного и пассивного сетевого оборудования (телекоммуникационного) и оборудования структурированных кабельных систем;

Система управления базами данных (СУБД) – совокупность программных и языковых средств, обеспечивающих управление БД;

Системное ПО – совокупность компьютерных программ для обеспечения работы вычислительного оборудования;

Системный администратор (СА) – лицо, ответственное за правильное функционирование сервера и настройки ПО на сервере;

Специализированное ПО – компьютерные программы, применяемые для решения вспомогательных и сервисных задач;

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 8 из 13

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки информации, в том числе ввода или вывода, способных функционировать самостоятельно или в составе других систем;

Сеть интернет – система сетей, обеспечивающая доступ к международным ресурсам.

4. ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основными объектами защиты ИБ университета являются:

- 1) ИР с ограниченным доступом, составляющие тайну, чувствительные по отношению к несанкционированным воздействиям и нарушению их безопасности, в том числе открытая (общедоступная) информация, независимо от формы и вида представления;
- 2) процессы и человеческие ресурсы обработки информации в ИС - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков, внутренние пользователи системы и ее обслуживающий персонал;
- 3) информационная инфраструктура, включающая системы обработки и анализа информации, передачи и отображения, в том числе каналы информационного обмена, объекты и помещения, в которых размещены ИР и компоненты ИС.

5. ОРГАНИЗАЦИОННО-ПРАВОВОЙ СТАТУС ОТВЕТСТВЕННОГО ЛИЦА ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

5.1 Ответственное лицо за ИБ имеет необходимые права:

- 1) мониторинга и контроля информационной инфраструктуры университета;
- 2) доступа во все помещения университета, где установлена ИС, СВТ и ЛВС университета;
- 3) прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации.

5.2. СА по согласованию с ответственным лицом за ИБ имеют право:

- 1) доступа во все помещения университета, где установлена ИС, СВТ и ЛВС университета;
- 2) прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации.

6. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Общие требования конфиденциальности

6.1.1. Главными требованиями конфиденциальности являются предотвращение утечки (разглашения) какой-либо конфиденциальной информации и обеспечение предоставления информации только авторизованным лицам.

6.1.2. Подключения внутренних пользователей к ИС университета должны фиксироваться в полном и тщательном виде с сохранением данной информации (логирование) на срок не более 1 года.

6.1.3. Служебная и иная защищаемая информация, обрабатываемая и хранящаяся в ИС университета, подлежит копированию и передаче третьему лицу только с официального разрешения курирующего проректора-члена Правления.

6.1.4. При работе с ИС университета должна исключаться возможность наблюдения за отображаемой информацией на экране монитора внутреннего пользователя посторонними лицами.

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 9 из 13

6.1.5. При работе ИС университета должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак. Для защиты от нелегального внедрения и использования неучтенных программ в университет, кроме мероприятий, включающих физическую защиту, должен проводиться мониторинг системных журналов, на рабочие станции внутренних пользователей должен устанавливаться базовый комплекс ПО. В базовый комплекс ПО включается лицензионное ПО, необходимое для обеспечения работоспособности СВТ.

6.1.6. Соблюдение требований конфиденциальности внутренними пользователями и вспомогательным персоналом при работе с ИС университета должно обеспечиваться соглашением о конфиденциальности.

7. ТРЕБОВАНИЯ ПО АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ

Все внутренние пользователи, работающие в ИС университета, должны проходить безопасную аутентификацию исключающую возможность утечки и перехвата авторизованных данных.

Для аутентификации внутренних пользователей в ИС создаются уникальные идентификационные учетные записи (логин, пароль).

Ответственность за сохранность и неразглашение сведений об учетной записи возлагается на самих внутренних пользователей ИС.

Учетные записи внутренних пользователей должны создаваться и удаляться только при наличии соответствующих документов или записей.

Требования к организации парольной защиты действиям внутренних пользователей и обслуживающего персонала ИС при работе с паролями, личный пароль должен быть не менее 8 символов и не включать слова из общего словаря, при этом включать минимум три следующих набора символов:

а) заглавных букв: А, В, С;

б) маленьких букв: а, б, с;

в) цифр: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9;

г) символов: '~!@#%&'()*_+ = { } | \ :

Требования конфиденциальности при передаче информации по линиям связи

Передача информации университета должна осуществляться по собственным либо арендуемым волоконно-оптическим каналам, на больших расстояниях.

Серверное, телекоммуникационное оборудование и структурированная кабельная система должны иметь документальное подтверждение соответствия требованиям в области технического регулирования и иметь сертификат соответствия требованиям ИБ.

Не рекомендуются использовать почтовые адреса электронной почты университета при регистрации на сайтах и при участии в форумах или интернет-конференциях (за исключением случаев, когда это относится к мероприятиям, связанным с профессиональной деятельностью сотрудника).

Не рекомендуются общедоступные почтовые сервисы Интернета и Интернет- системы мгновенного общения сотрудникам, работающим с конфиденциальной информацией.

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 10 из 13

8. ПЕРЕСМОТР ПОЛОЖЕНИЯ

- 8.1. Развитие, пересмотр и оценку Положения осуществляет ответственное лицо за ИБ на основе ежегодного анализа и оценки рисков ИБ.
- 8.2. Пересмотр Положения производится в целях:
- усовершенствования целей и мер контроля ИБ;
 - усовершенствования подхода к управлению ИБ и бизнес-процессами университета;
 - улучшения распределения ресурсов и/или обязанностей.
- 8.3. Положение должно пересматриваться в соответствии с изменениями, влияющими на основу первоначальной оценки риска, путем выявления существенных инцидентов нарушения ИБ, появления новых уязвимостей или изменения организационной/технологической инфраструктуры, изменении основных характеристик бизнес-процессов университета.
- 8.4. В случае появления существенных изменений в технологиях, обеспечивающих ИБ, в целях обеспечения конфиденциальности, целостности, доступности информации, а также адекватности и эффективности применяемых мер ИБ.
- 8.5. В случае возникновения дополнительных замечаний и предложений со стороны внутренних и внешних пользователей к изменениям норм Положения данные предложения анализируются ответственным лицом за ИБ и при необходимости вносятся для утверждения.
- 8.6. Руководством университета может инициироваться независимый пересмотр Положения. Такой пересмотр проводится лицом, не имеющим прямого отношения к пересматриваемой области безопасности, например, функция внутреннего аудита осуществляется независимым менеджером или организацией третьей стороны, специализирующейся на таких пересмотрах. Результаты независимого пересмотра документируются в виде отчета и доводятся до сведения председателя Правления университета.
- 8.7. Положение должно быть пересмотрено после проведения анализа и оценки рисков ИБ для университета, по итогам которых, с учетом исправления выявленных недостатков необходима ее актуализация.
- 8.8. Пересмотр Положения ИБ должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации».

9. ОТВЕТСТВЕННОСТЬ

- 9.1. Ответственное лицо за ИБ совместно с курирующим проректором-членом Правления университета обеспечивает:
- 1) определение целей ИБ в соответствии с организационными требованиями и интеграцией в бизнес-процессы университета;
 - 2) контроль выполнения всех пунктов настоящего Положения ИБ;
 - 3) четкое управление и зримую поддержку инициатив в области поддержки ИБ университета;
 - 4) предоставление ресурсов для обеспечения ИБ;
 - 5) контроль издания и доведения до сведения утвержденных документов до пользователей ИКИ университета.
- 9.2. Курирующий проректор университета по представлению ответственного лица за ИБ должен:
- 1) согласовывать разрабатываемые, пересматриваемые правовые документы по ИБ университета;

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 11 из 13

- 2) вести контроль за эффективностью реализации Положения ИБ;
- 3) утверждать распределение специфических ролей и обязанностей по ИБ;
- 4) инициировать планы и программы по осведомлённости об ИБ;
- 9.3. Руководители структурных подразделений университета несут ответственность за выполнение требований Положения, а также за ознакомление с настоящим Положением своих подчиненных, в том числе вновь принятых сотрудников.
- 9.4. При нарушении требований Положения, повлекших за собой моральный и материальный ущерб для университета, причастные сотрудники привлекаются к ответственности в соответствии с законодательством Республики Казахстан.
- 9.5. Нарушение требований настоящего Положения квалифицируется как дисциплинарный проступок, заключающийся в неисполнении или ненадлежащем исполнении трудовых обязанностей. Сотрудник, допустивший нарушение требований Положения ИБ, привлекается к дисциплинарной ответственности в соответствии с Трудовым кодексом Республики Казахстан и требованием пунктов 8.2.3 и 13.2.3 Государственного стандарта СТ РК ИСО/МЭК 27002-2009 «Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации».
- 9.6. Пользователи ИС Учреждения несут персональную ответственность за несоблюдение требований по парольной защите.
- 9.7. Администратор АИС несет ответственность за компрометацию и нецелевое использование привилегированных учетных записей.
- 9.8. Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам ИС Учреждения действиями либо бездействием соответствующего пользователя.

10. ЗАКЛЮЧИТЕЛЬНОЕ ПОЛОЖЕНИЕ

Внесение изменений и дополнений в настоящее Положение осуществляется только по разрешению проректора по академическим вопросам и оформляется документально за его подписью. Внесение изменений и дополнений в подлинник и учетные рабочие экземпляры производится в соответствии с требованиями Положения о порядке разработки положений. За внесение изменений и дополнений в подлинник и учетные рабочие экземпляры несет ответственность РСП.

Положение пересматривается по мере необходимости.

Основанием для внесения изменений и дополнений в Положение может являться:

- вновь введенные изменения и дополнения в нормативно-правовые акты, имеющие силу закона;
- приказы Председателя правления-ректора;
- перераспределение обязанностей между структурными подразделениями;
- реорганизация структурных подразделений;
- при изменении названия организации или структурного подразделения Положение должен быть заменен.

В случае замены все имеющиеся в университете экземпляры утратившего силу Положение должны быть изъяты и заменены новыми.

Согласование Положения в соответствии с требованиями нормативно-правовых актов Республики Казахстан осуществляет ОМК.

 ATYRAU UNIVERSITY	Атырауский университет имени Халела Досмухамедова	Издание: первое
	ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)	Стр. 12 из 13

Ответственность за замену и изъятие утратившего силу Положения несут РСП.
 Ответственность за хранение учтённого рабочего экземпляра Положения в подразделении несёт РСП.



Атырауский университет
имени Халела Досмухамедова

Издание:
первое

ПОЛОЖЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РАБОТЕ С АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (АИС)

Стр. 13 из 13

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

[illegible]